4. Active Reconnaissance

🔎 Active Reconnaissance & Essential Tools

1. What is Active Reconnaissance?

- **Definition:** Active reconnaissance involves **directly interacting with the target system or network** to gather information.
- Methods include:
  - **Port scanning** (e.g., Nmap)
  - **Banner grabbing** (to identify software versions)
  - **Ping sweeps**
  - **Service probing**
- It **sends packets or requests** to the target and analyzes responses.
- Provides **accurate and detailed info**, but risks detection.

2. Why is Active Reconnaissance Important for Cybersecurity?

- **Accurate asset identification:** Finds open ports, active services, and software versions that passive methods might miss.
- **Vulnerability identification:** Helps determine exploitable services or software bugs.
- **Penetration Testing:** Essential for building attack strategies.
- **Security Assessment:** Helps defenders understand real exposure and patch gaps.
- **Incident Response:** Identifies compromised hosts and attacker activity.

⚠️ Must be done with authorization to avoid legal issues.

3. How Can Wappalyzer Be Used for Active Reconnaissance?

- **Wappalyzer** is a tool (browser extension & CLI) that identifies **technologies used on websites** (CMS, frameworks, web servers, analytics, etc.).
- When browsing or scanning a web target:
  - It **actively probes website responses** to detect headers, scripts, meta tags.
  - Reveals tech stack — e.g., WordPress, React, Apache, Nginx, PHP versions.
- Helps **understand attack surface** and **technology-specific vulnerabilities**.
- Can be automated for multiple URLs during active recon.

4. What is DNS Enumeration?

- DNS enumeration is the process of **discovering DNS information** about a domain.
- Goal: Identify **hostnames, subdomains, IP addresses, mail servers**, and other related info.
- Techniques include:
  - Zone transfers (if misconfigured)
  - Brute forcing subdomains with wordlists
  - Querying DNS records (`A`, `MX`, `NS`, `TXT`)
  - Passive methods using OSINT tools and public databases.

---

5. How to Enumerate SMTPs Using Command-Line Tools?

- SMTP servers handle email sending/receiving. Enumeration helps find **mail servers** and test for vulnerabilities.
- Use tools like:
  - `nslookup` or `dig` to get **MX records**:

    ```
    dig example.com MX
    ```

  - **Telnet or Netcat** to connect to SMTP port (usually 25):

    ```
    telnet mail.example.com 25
    ```

  - After connecting, use SMTP commands like `VRFY` (verify email addresses) or `EXPN` (expand mailing lists) to enumerate users (if server allows).
- Example workflow:

```
dig example.com MX
telnet mx1.example.com 25
HELO attacker.com
VRFY admin
```

- Note: Many SMTP servers disable VRFY and EXPN for security.

---

6. How Should We Perform OS Fingerprinting?

- OS fingerprinting determines the **operating system running on a target host** by analyzing network responses.
- Types:
  - **Active fingerprinting:** Send crafted packets and analyze responses (e.g., Nmap TCP/IP stack fingerprinting).
  - **Passive fingerprinting:** Analyze network traffic without sending packets (e.g., observing TTL, window size).
- Tools:

- `nmap -O <target_ip>` (active)
- `p0f` (passive)

- Results help tailor attacks or defenses.

---

7. What is sqlmap? How to Use It?

- **sqlmap** is an open-source automated tool to detect and exploit **SQL injection vulnerabilities** in web applications.
- Features:
  - Supports various databases (MySQL, PostgreSQL, MSSQL, Oracle, etc.)
  - Automates injection detection, exploitation, and database enumeration
  - Can extract data, execute commands, upload files, and even get shell access.

Basic usage:

```
sqlmap -u "http://target.com/page.php?id=1" --batch --dbs
```

- `-u` specifies the target URL with injectable parameter.
- `--batch` runs non-interactively using default options.
- `--dbs` lists the databases available.

Further options:

- `--tables` to list tables.
- `--dump` to extract data.
- `--os-shell` to attempt OS-level shell access.
